

What Is Claimed Is:

1 1. A method for resolving conflicts between network service rules for
2 network data traffic in a system where rule patterns with longer prefixes match
3 before rule patterns with shorter prefixes, comprising:

4 receiving a set of network service rules for network data traffic from
5 multiple network services, wherein network service rules from different network
6 services can possibly conflict;

7 wherein each of the network service rules specifies, a filter that defines a
8 prefix for a set of packets in the packet flow, and an action list that specifies one
9 or more actions to be applied to the set of packets;

10 identifying a conflict between a higher priority rule and a lower priority
11 rule in the set of network service rules; and

12 resolving the conflict by prepending an action list of the higher priority
13 rule to an action list of a rule with a filter that defines a longer prefix.

1 2. The method of claim 1, wherein if the set of packets associated
2 with the higher priority rule is equal to the set of packets associated with the lower
3 priority rule, resolving the conflict involves creating a new action list for the
4 higher priority rule by prepending the action list of the higher priority rule to the
5 action list of the lower priority rule.

1 3. The method of claim 1, wherein if the set of packets associated
2 with the higher priority rule is a superset of the set of packets associated with the
3 lower priority rule, resolving the conflict involves creating a new action list for
4 the lower priority rule by prepending the action list of the higher priority rule to
5 the action list of the lower priority rule.

1 4. The method of claim 1, wherein if the set of packets associated
2 with the lower priority rule is a superset of the set of packets associated with the
3 higher priority rule, resolving the conflict involves creating a new action list for
4 the higher priority rule by prepending the action list of the higher priority rule to
5 the action list of the lower priority rule.

1 5. The method of claim 1, wherein if the set of packets associated
2 with the lower priority rule intersects the set of packets associated with the higher
3 priority rule, resolving the conflict involves:
4 creating a new rule with a filter that defines the intersection of the set of
5 packets associated with lower priority rule and the set of packets associated with
6 the higher priority rule; and
7 creating an action list for the new rule by prepending the action list of the
8 higher priority rule to the action list of the lower priority rule.

1 6. The method of claim 1, wherein prior to modifying a rule in the set
2 of network service rules, the method further comprises cloning the rule to ensure
3 that potential conflicts with rules that appear later in the set of network service
4 rules are not overlooked.

1 7. The method of claim 1, wherein the priority of a given rule is based
2 upon one or more of the following:
3 a priority associated with a network service from which given rule
4 originated;
5 a count of the number of prefix bits specified by the filter for the given
6 rule; and

7 a time stamp indicating when the given rule was incorporated into the set
8 of network service rules.

1 8. The method of claim 1, wherein an action specified by a network
2 service rule can include, but is not limited to:

3 dropping a packet;
4 gathering statistical information about the packet;
5 controlling timer functions associated with the packet;
6 modifying the packet; and
7 passing the packet on.

1 9. The method of claim 1, wherein the multiple network services can
2 include, but is not limited to:

3 a firewall service;
4 a service level agreement monitoring service;
5 a load balancing service;
6 a transport matching service;
7 a failover service; and
8 a high availability service.

1 10. A computer-readable storage medium storing instructions that
2 when executed by a computer cause the computer to perform a method for
3 resolving conflicts between network service rules for network data traffic in a
4 system where rule patterns with longer prefixes match before rule patterns with
5 shorter prefixes, the method comprising:

6 receiving a set of network service rules for network data traffic from
7 multiple network services, wherein network service rules from different network
8 services can possibly conflict;

9 wherein each of the network service rules specifies, a filter that defines a
10 prefix for a set of packets in the packet flow, and an action list that specifies one
11 or more actions to be applied to the set of packets;

12 identifying a conflict between a higher priority rule and a lower priority
13 rule in the set of network service rules; and

14 resolving the conflict by prepending an action list of the higher priority
15 rule to an action list of a rule with a filter that defines a longer prefix.

1 11. The computer-readable storage medium of claim 10, wherein if the
2 set of packets associated with the higher priority rule is equal to the set of packets
3 associated with the lower priority rule, resolving the conflict involves creating a
4 new action list for the higher priority rule by prepending the action list of the
5 higher priority rule to the action list of the lower priority rule.

1 12. The computer-readable storage medium of claim 10, wherein if the
2 set of packets associated with the higher priority rule is a superset of the set of
3 packets associated with the lower priority rule, resolving the conflict involves
4 creating a new action list for the lower priority rule by prepending the action list
5 of the higher priority rule to the action list of the lower priority rule.

1 13. The computer-readable storage medium of claim 10, wherein if the
2 set of packets associated with the lower priority rule is a superset of the set of
3 packets associated with the higher priority rule, resolving the conflict involves

4 creating a new action list for the higher priority rule by prepending the action list
5 of the higher priority rule to the action list of the lower priority rule.

1 14. The computer-readable storage medium of claim 10, wherein if the
2 set of packets associated with the lower priority rule intersects the set of packets
3 associated with the higher priority rule, resolving the conflict involves:

4 creating a new rule with a filter that defines the intersection of the set of
5 packets associated with lower priority rule and the set of packets associated with
6 the higher priority rule; and

7 creating an action list for the new rule by prepending the action list of the
8 higher priority rule to the action list of the lower priority rule.

1 15. The computer-readable storage medium of claim 10, wherein prior
2 to modifying a rule in the set of network service rules, the method further
3 comprises cloning the rule to ensure that potential conflicts with rules that appear
4 later in the set of network service rules are not overlooked.

1 16. The computer-readable storage medium of claim 10, wherein the
2 priority of a given rule is based upon one or more of the following:

3 a priority associated with a network service from which given rule
4 originated;

5 a count of the number of prefix bits specified by the filter for the given
6 rule; and

7 a time stamp indicating when the given rule was incorporated into the set
8 of network service rules.

1 17. The computer-readable storage medium of claim 10, wherein an
2 action specified by a network service rule can include, but is not limited to:
3 dropping a packet;
4 gathering statistical information about the packet;
5 controlling timer functions associated with the packet;
6 modifying the packet; and
7 passing the packet on.

1 18. The computer-readable storage medium of claim 10, wherein the
2 multiple network services can include, but is not limited to:
3 a firewall service;
4 a service level agreement monitoring service;
5 a load balancing service;
6 a transport matching service;
7 a failover service; and
8 a high availability service.

1 19. An apparatus that resolves conflicts between network service rules
2 for network data traffic in a system where rule patterns with longer prefixes match
3 before rule patterns with shorter prefixes, comprising:
4 a receiving mechanism configured to receive a set of network service rules
5 for network data traffic from multiple network services, wherein network service
6 rules from different network services can possibly conflict;
7 wherein each of the network service rules specifies, a filter that defines a
8 prefix for a set of packets in the packet flow, and an action list that specifies one
9 or more actions to be applied to the set of packets;

10 a conflict detection mechanism configured to identify a conflict between a
11 higher priority rule and a lower priority rule in the set of network service rules;
12 and

13 a conflict resolution mechanism configured to resolve the conflict by
14 prepend an action list of the higher priority rule to an action list of a rule with a
15 filter that defines a longer prefix.

1 20. The apparatus of claim 19, wherein if the set of packets associated
2 with the higher priority rule is equal to the set of packets associated with the lower
3 priority rule, the conflict resolution mechanism is configured to:

4 create a new action list for the higher priority rule by prepending the action
5 list of the higher priority rule to the action list of the lower priority rule; and to
6 delete the lower priority rule.

1 21. The apparatus of claim 19, wherein if the set of packets associated
2 with the higher priority rule is a superset of the set of packets associated with the
3 lower priority rule, the conflict resolution mechanism is configured to create a
4 new action list for the lower priority rule by prepending the action list of the
5 higher priority rule to the action list of the lower priority rule.

1 22. The apparatus of claim 19, wherein if the set of packets associated
2 with the lower priority rule is a superset of the set of packets associated with the
3 higher priority rule, the conflict resolution mechanism is configured to create a
4 new action list for the higher priority rule by prepending the action list of the
5 higher priority rule to the action list of the lower priority rule.

1 23. The apparatus of claim 19, wherein if the set of packets associated
2 with the lower priority rule intersects the set of packets associated with the higher
3 priority rule, the conflict resolution mechanism is configured to:

4 create a new rule with a filter that defines the intersection of the set of
5 packets associated with lower priority rule and the set of packets associated with
6 the higher priority rule; and to

7 create an action list for the new rule by prepending the action list of the
8 higher priority rule to the action list of the lower priority rule.

1 24. The apparatus of claim 19, wherein prior to modifying a rule in the
2 set of network service rules, the conflict resolution mechanism is configured to
3 clone the rule to ensure that potential conflicts with rules that appear later in the
4 set of network service rules are not overlooked.

1 25. The apparatus of claim 19, wherein the priority of a given rule is
2 based upon one or more of the following:

3 a priority associated with a network service from which given rule
4 originated;

5 a count of the number of prefix bits specified by the filter for the given
6 rule; and

7 a time stamp indicating when the given rule was incorporated into the set
8 of network service rules.

1 26. The apparatus of claim 19, wherein an action specified by a
2 network service rule can include, but is not limited to:

3 dropping a packet;
4 gathering statistical information about the packet;

5 controlling timer functions associated with the packet;
6 modifying the packet; and
7 passing the packet on.

1 27. The apparatus of claim 19, wherein the multiple network services
2 can include, but is not limited to:

3 a firewall service;
4 a service level agreement monitoring service;
5 a load balancing service;
6 a transport matching service;
7 a failover service; and
8 a high availability service.